

FIG. 1B

FIG. 1A

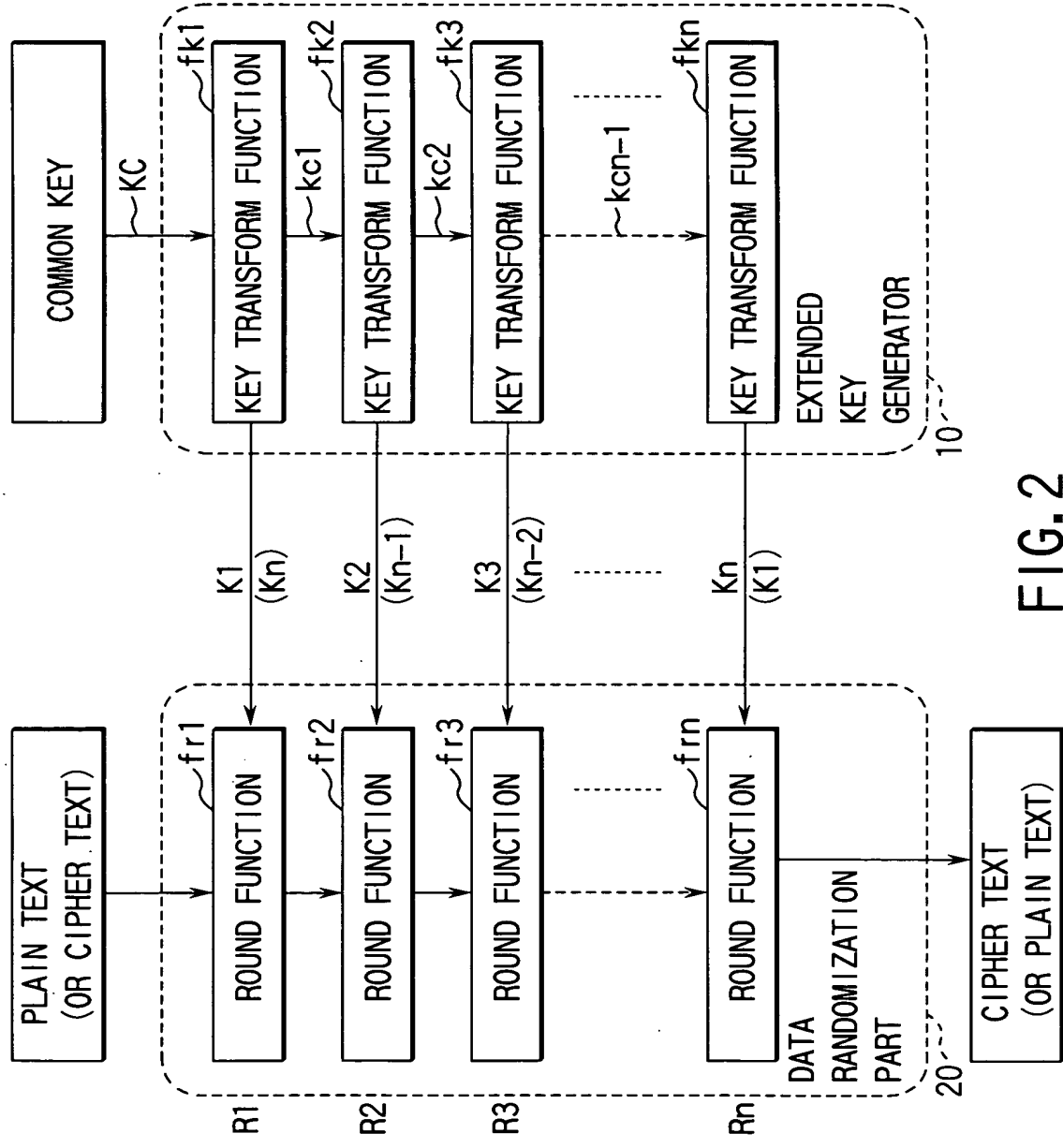


FIG. 2

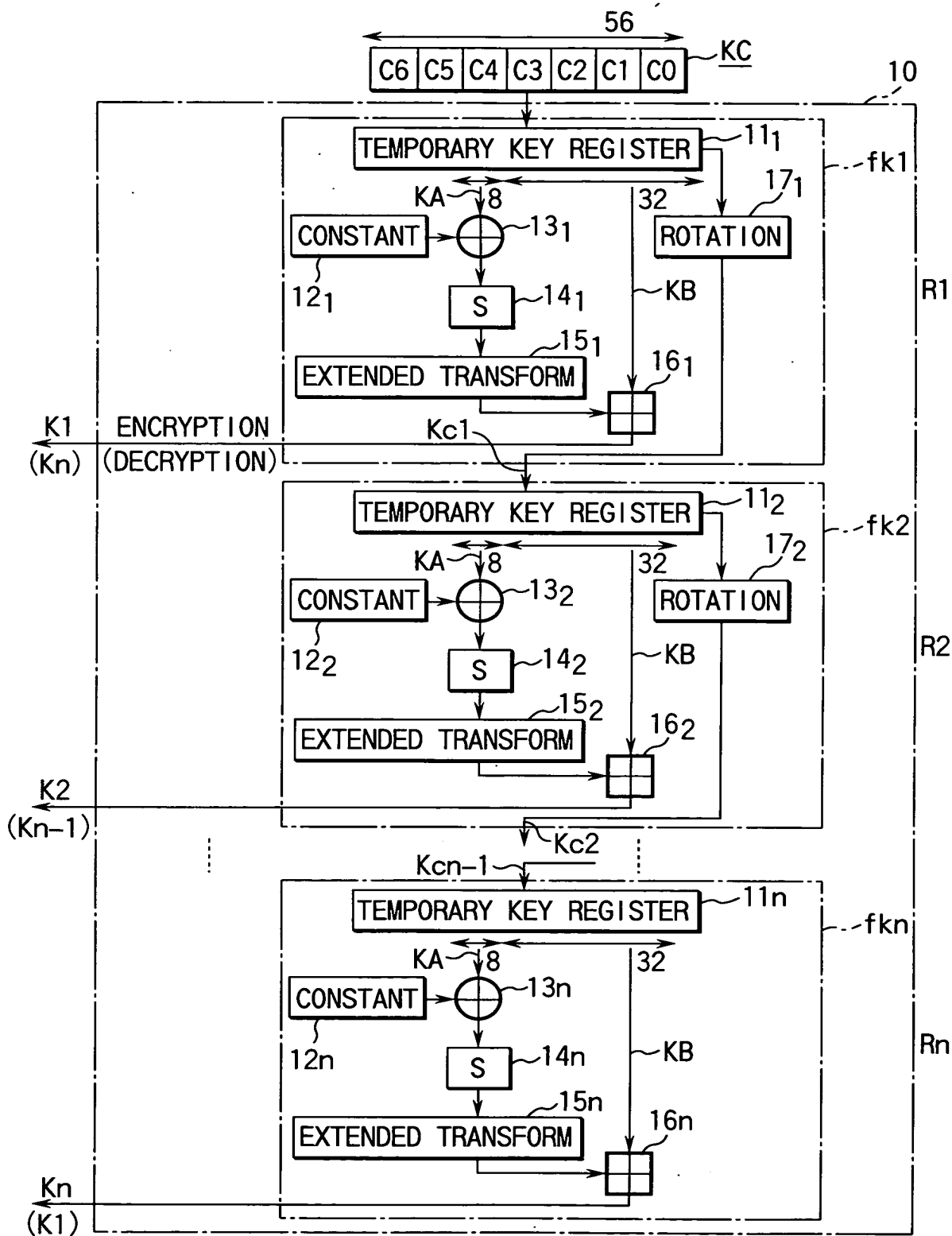


FIG. 3

KEY TRTRANSFORM FUNCTION f _k i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
VALUE OF CONSTANT REGISTER	0	1	2	3	4	5	6	7	7	6	5	4	3	2	1	0

FIG. 4A

KEY TRTRANSFORM FUNCTION f _k i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
VALUE OF CONSTANT	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
REGISTER DECRYPTION	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

FIG. 4B

48,	54,	216,	182,	175,	5,	130,	229,	107,	52,	86,	11,	12,	221,	14,	15,
59,	4,	41,	140,	22,	164,	7,	89,	124,	81,	225,	176,	101,	66,	30,	118,
126,	242,	44,	211,	18,	161,	249,	105,	222,	174,	141,	202,	34,	103,	87,	233,
71,	49,	187,	51,	39,	1,	91,	77,	181,	172,	55,	42,	199,	79,	62,	194,
64,	72,	68,	133,	190,	158,	165,	232,	231,	115,	186,	116,	217,	240,	129,	171,
74,	169,	204,	173,	57,	58,	93,	17,	159,	245,	241,	155,	92,	156,	94,	26,
132,	82,	109,	230,	227,	28,	131,	209,	170,	25,	106,	73,	85,	98,	128,	143,
237,	108,	160,	61,	21,	179,	254,	197,	38,	122,	235,	70,	125,	31,	40,	102,
246,	119,	207,	53,	214,	111,	63,	135,	184,	236,	138,	56,	19,	29,	213,	88,
144,	145,	243,	127,	148,	137,	189,	151,	78,	153,	123,	183,	114,	157,	255,	252,
33,	6,	147,	163,	84,	97,	166,	167,	192,	0,	10,	208,	117,	196,	9,	16,
27,	206,	177,	104,	195,	83,	24,	75,	150,	203,	188,	50,	100,	69,	20,	180,
134,	193,	168,	8,	251,	247,	149,	201,	200,	112,	43,	142,	139,	205,	212,	37,
60,	226,	210,	154,	239,	80,	244,	215,	3,	120,	45,	23,	67,	99,	219,	223,
250,	220,	191,	32,	185,	253,	121,	13,	36,	228,	96,	162,	136,	46,	238,	146,
110,	178,	152,	2,	90,	234,	95,	65,	248,	113,	224,	35,	76,	218,	198,	47,

FIG. 5

NUMBER OF ROUNDS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ENCRYPTION (LEFT ROTATION)	9	9	11	11	13	13	13	10	13	13	13	11	11	9	9	9
DECRYPTION (RIGHT ROTATION)	9	9	11	11	13	13	13	10	13	13	13	11	11	9	9	9
KEY TRANSFORM FUNCTION f_{ki}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	15

FIG.6

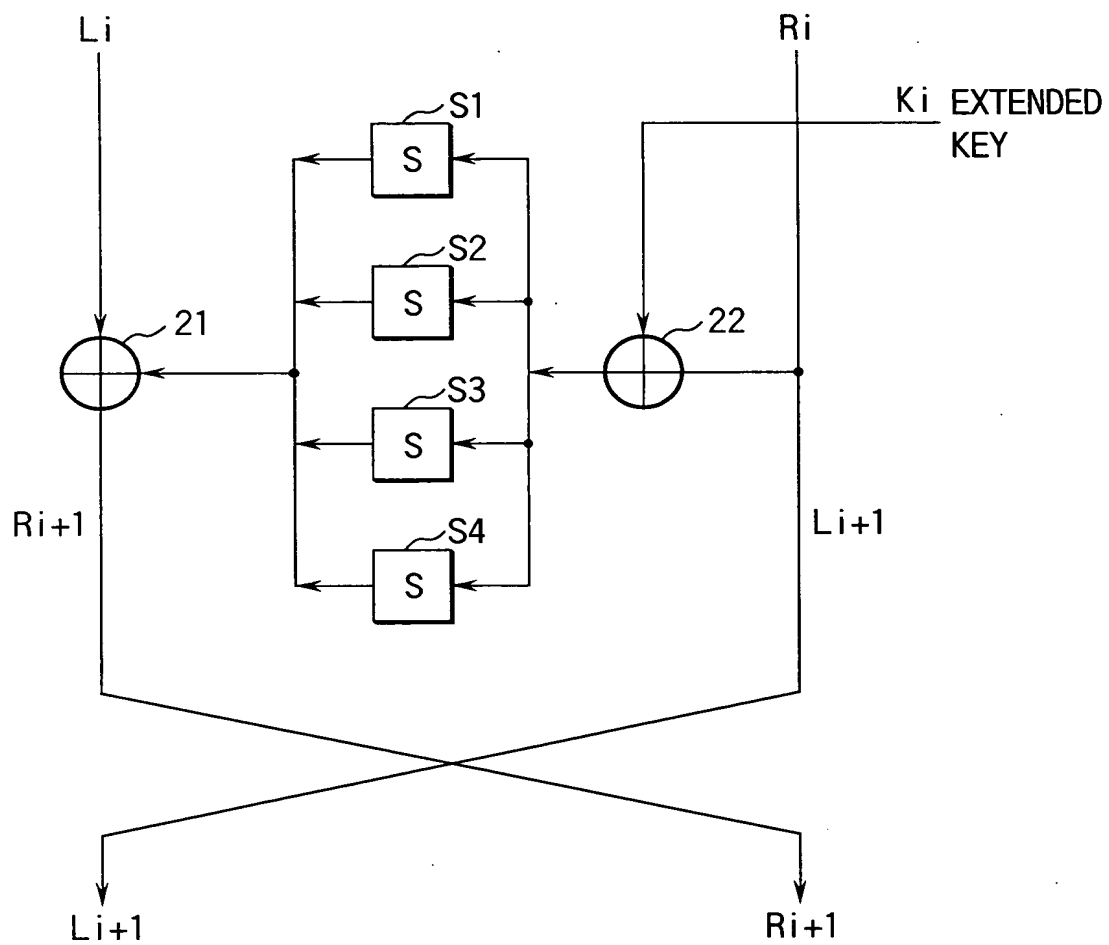


FIG. 7

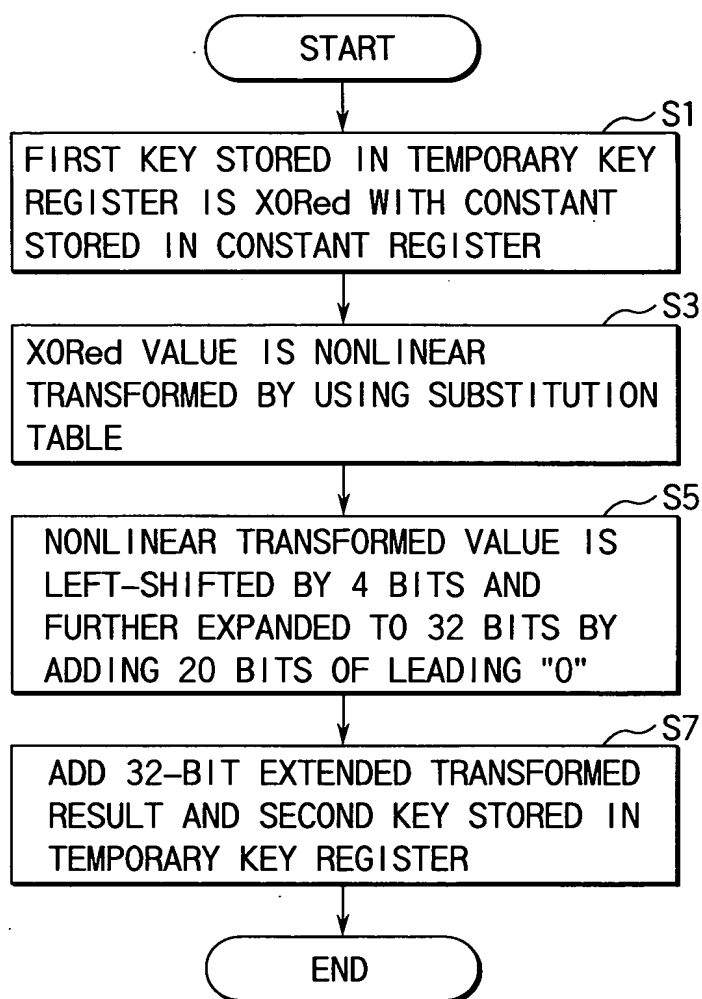


FIG. 8

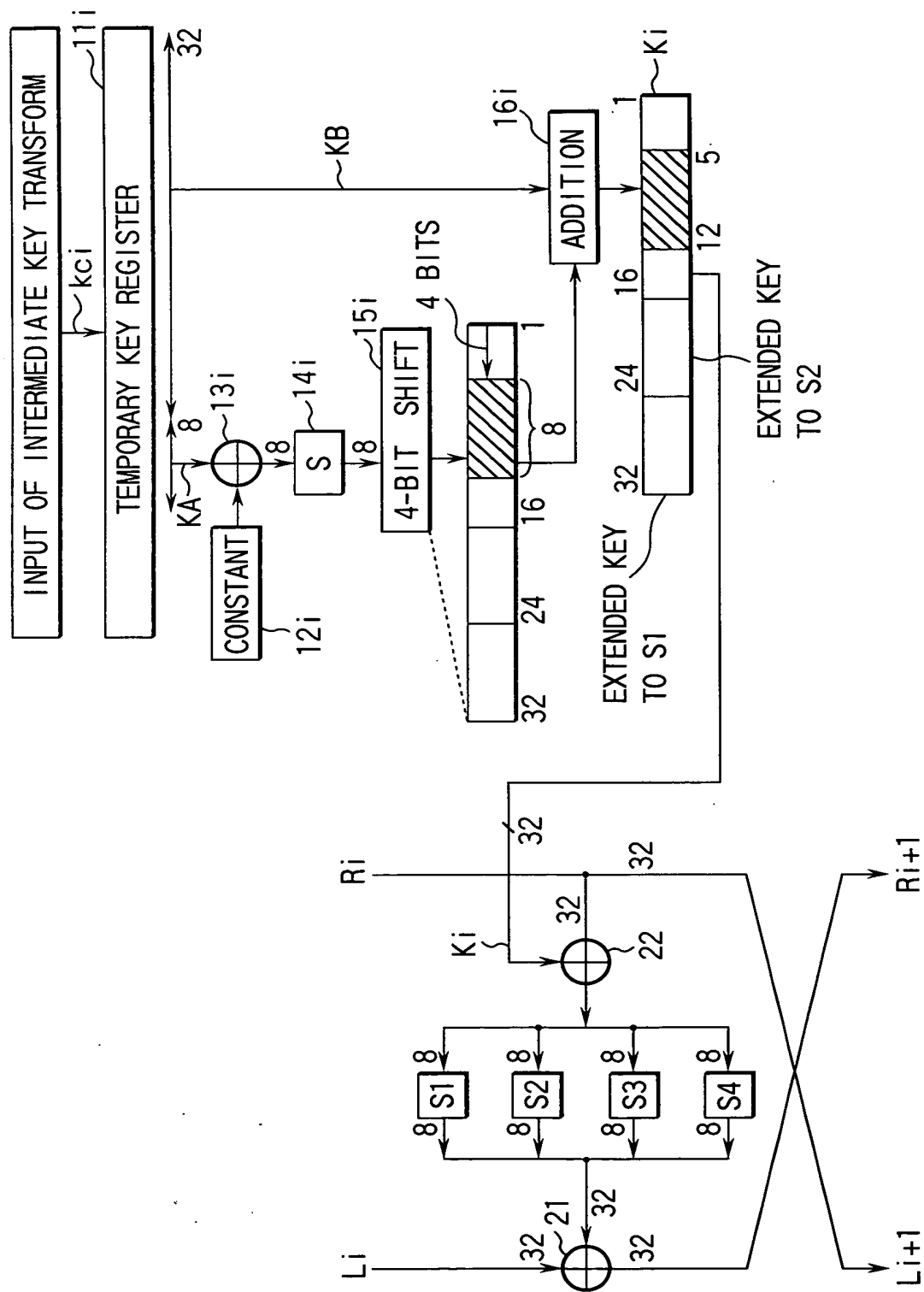


FIG. 9

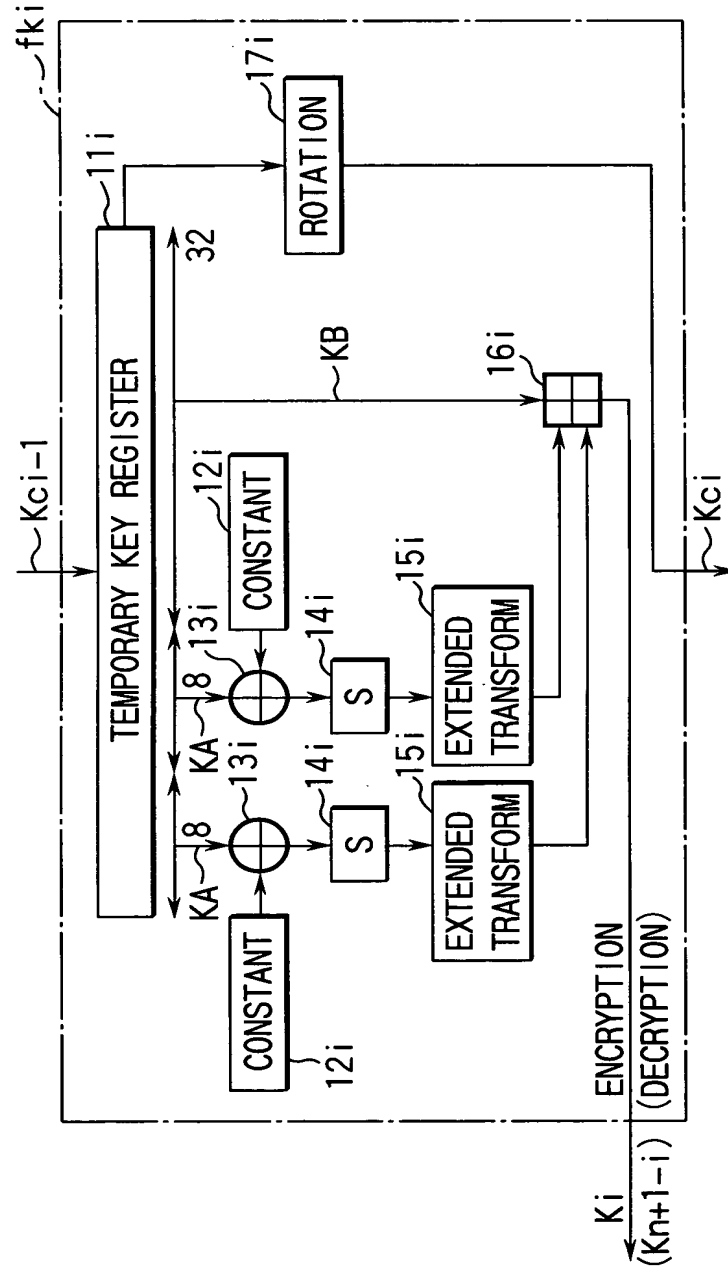


FIG. 10

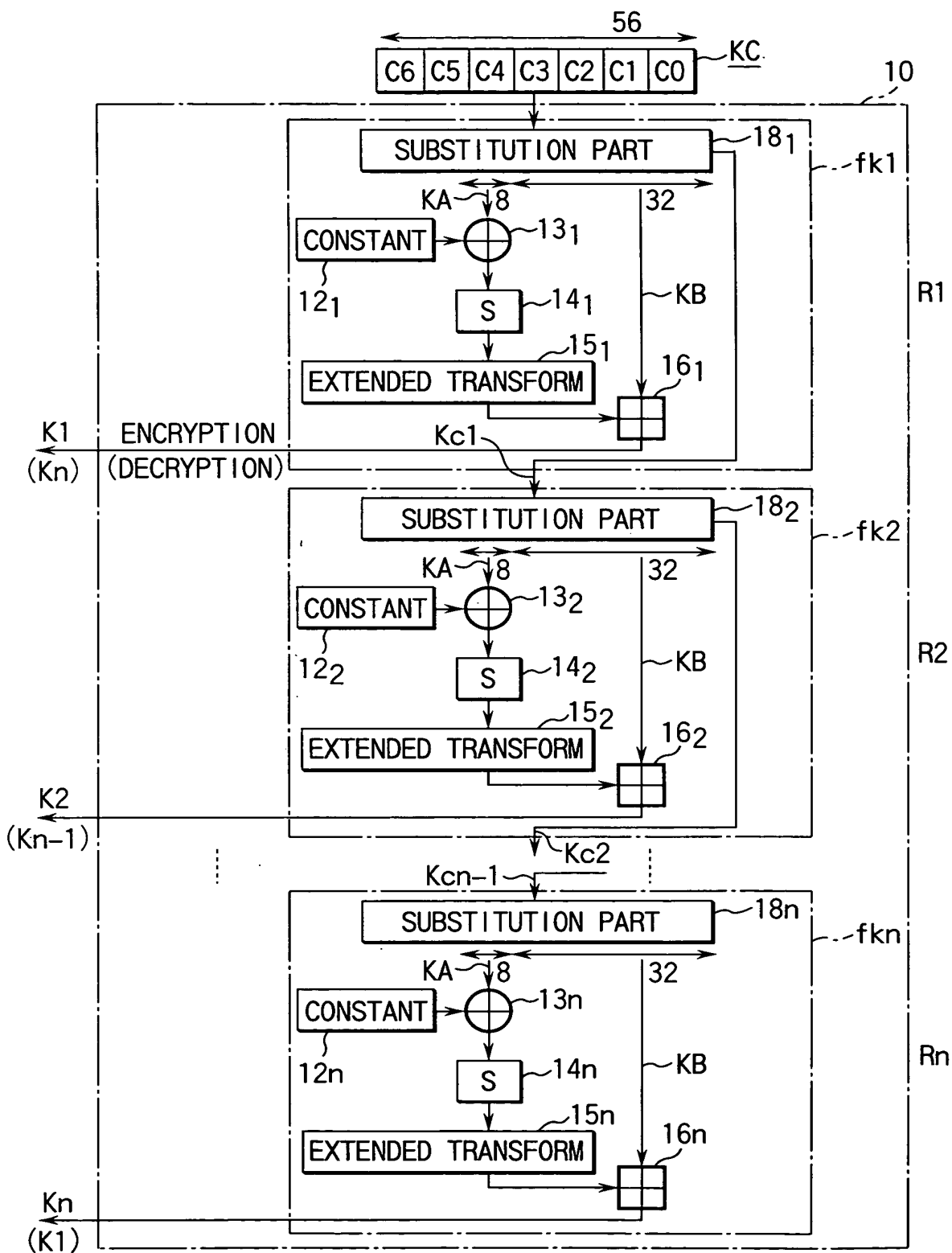


FIG. 11

NUMBER OF ROUNDS		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
		ENCRYPTION	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
PERMUTATION INPUT PROCESS	DECRYPTION	P16 ⁻¹	P15 ⁻¹	P14 ⁻¹	P13 ⁻¹	P12 ⁻¹	P11 ⁻¹	P10 ⁻¹	P9 ⁻¹	P8 ⁻¹	P7 ⁻¹	P6 ⁻¹	P5 ⁻¹	P4 ⁻¹	P3 ⁻¹	P2 ⁻¹	P1 ⁻¹

FIG.12

```
graph TD; START([START]) --> S21[SUBSTITUTE COMMON KEY NONLINEARLY]; S21 --> S23[FIRST KEY OBTAINED FROM SUBSTITUTED KEY IS XORed WITH CONSTANT STORED IN CONSTANT REGISTER]; S23 --> S25[XORed VALUE IS NONLINEAR TRANSFORMED BY USING SUBSTITUTION TABLE]; S25 --> S27[NONLINEAR TRANSFORMED VALUE IS LEFT-SHIFTED BY 4 BITS AND FURTHER EXPANDED TO 32 BITS BY ADDING 20 BITS OF LEADING "0"]; S27 --> S29[ADD 32-BIT EXTENDED TRANSFORMED RESULT AND SECOND KEY OBTAINED FROM SUBSTITUTED KEY]; S29 --> END([END]);
```

The flowchart illustrates the second embodiment of the encryption process. It begins with a START terminal, followed by step S21: "SUBSTITUTE COMMON KEY NONLINEARLY". This leads to step S23: "FIRST KEY OBTAINED FROM SUBSTITUTED KEY IS XORed WITH CONSTANT STORED IN CONSTANT REGISTER". The next step is S25: "XORed VALUE IS NONLINEAR TRANSFORMED BY USING SUBSTITUTION TABLE". This is followed by step S27: "NONLINEAR TRANSFORMED VALUE IS LEFT-SHIFTED BY 4 BITS AND FURTHER EXPANDED TO 32 BITS BY ADDING 20 BITS OF LEADING '0'". The final processing step is S29: "ADD 32-BIT EXTENDED TRANSFORMED RESULT AND SECOND KEY OBTAINED FROM SUBSTITUTED KEY", which concludes at an END terminal.

FIG. 13

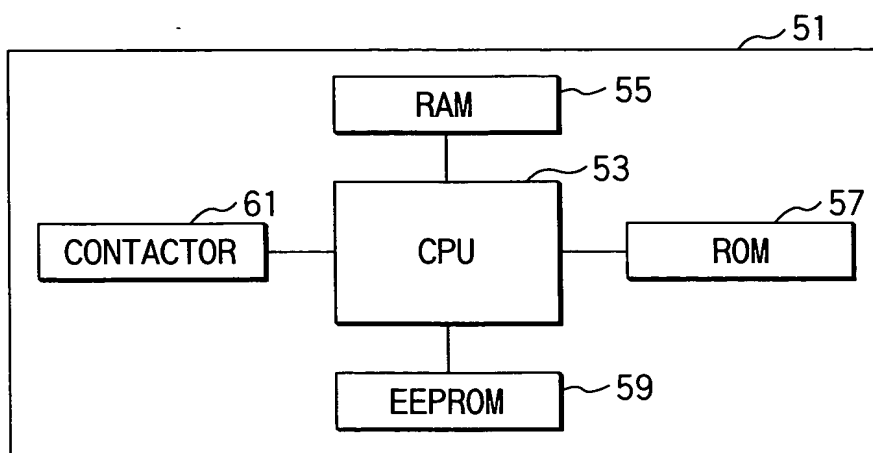


FIG. 14

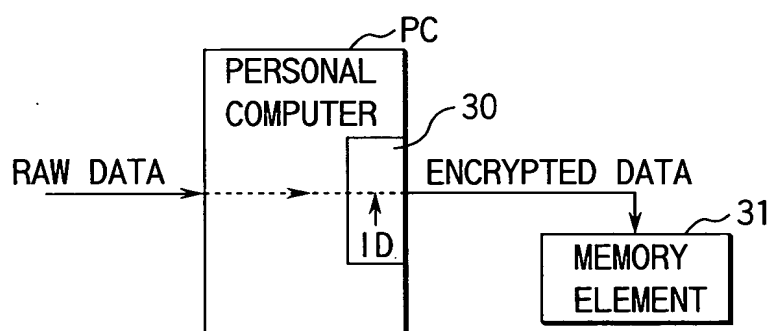


FIG. 15

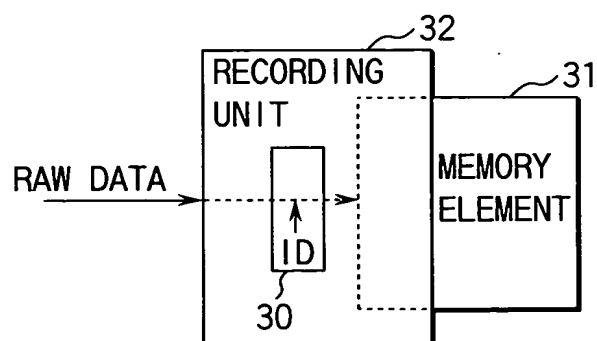


FIG. 16

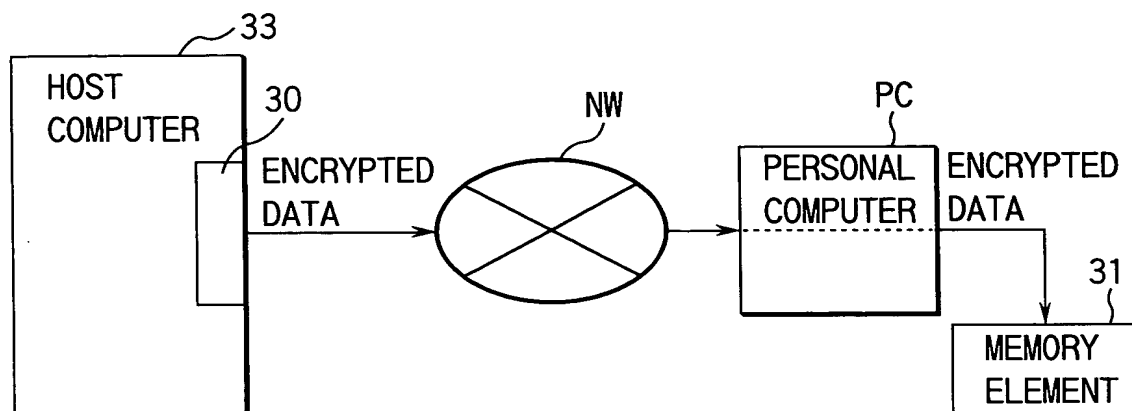


FIG. 17

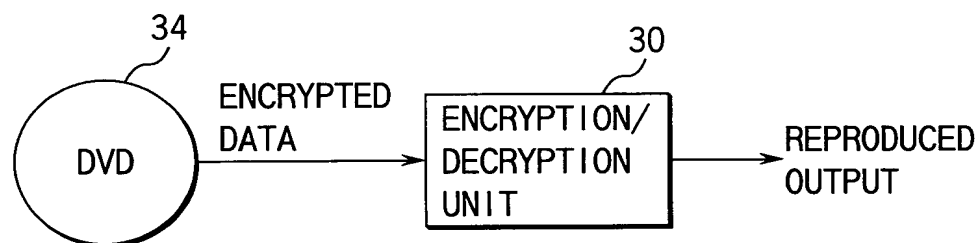


FIG. 18A

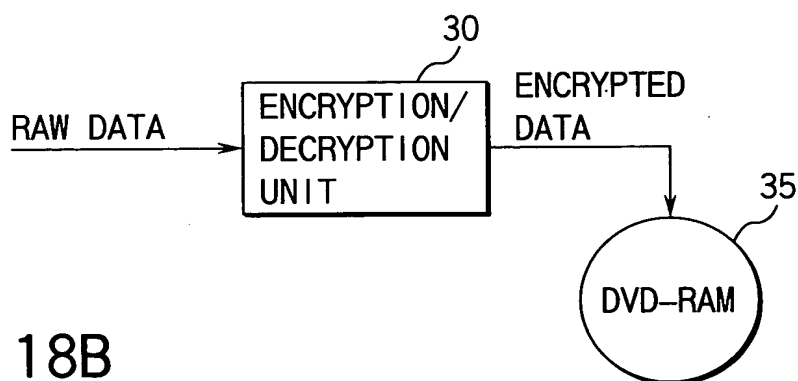


FIG. 18B